



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/646,398	08/21/2003	Eric J. Sprunk	018926-010010US	9498
7590		11/28/2007		
Robert P. Marley				
Motorola, Inc.				
Broadband Communications Sector				
101 Tournament Drive				
Horsham, PA 19044				
		EXAMINER		
		REZA, MOHAMMAD W		
		ART UNIT		PAPER NUMBER
		2136		
		MAIL DATE		DELIVERY MODE
		11/28/2007		PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/646,398	Applicant(s) SPRUNK, ERIC J.	
	Examiner Mohammad W. Reza	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 October 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-9, 11-15, 17 and 22-31 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-9, 11-15, 17, and 22-31 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This is in response to the RCE filed on 10/18/2007.
2. Claims 1-9, 11-15, 17, and 22-31 are pending in the application.
3. Claims 1-9, 11-15, 17, and 22-31 have been rejected.

Continued Examination Under 37 CFR 1.114

4. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 09/14/2006 has been entered.

Response to Amendment

5. The examiner does not approve the amendments made to claim 1, 12, and 22 as new matter introduced into the claims.
6. The examiner sustains the previous 112 rejection. The reason is given below.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1-9, 11-15, 17, and 22-31 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In these claims applicants mention **“provisioning information”**, **“first decryption information”**, **“first content”**, **“second decryption information”** which is generally narrative and indefinite with the invention. Applicants do not point out clearly which options include in the present invention by these terms. Examiner failed to understand what is the provisioning information and what does it include. According to the specification it seems, provisioning information is the unique identifier that generated during the subset configuration. If applicant does not agree on that then examiner requesting to provide the necessary explanation of what is the provisioning information. In the same way applicant featuring, **“first decryption information”**, **“first content”**, **“second decryption information”**. It is too broad to estimate what are the information includes in these terminologies. Are the **“first decryption information”**, **“second decryption information”** some kind of keys to decrypt any encrypted content or any information in decrypted form? Examiner also confused while the claim uses **“programs”** and **“first content”**? Why applicants call this content as **“first content”**? The examiner will interpret these words with the regarding claims as best understood

for applying the appropriate art for rejection purposes. Applicant also uses **“first method”** to encrypt the content by using the content encryption key? Why this encryption called as **“first method”**? Applicant argues that this amendment will help to withdraw the previous 112 rejection. However, examiner traverses this argument and maintains the previous 112 rejection. Furthermore, **“wherein the second decryption information is cryptographically secured with the first decryption information”**. What does it mean by cryptographically secured? It is too broad to understand the term **“cryptographically secured”**. Appropriate correction needs to overcome all these the rejections.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claims 1-9, 11-15, 17, and 22-31 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Applicant claimed the priority of a provisional application. The specifications of the both the provisional and current application does not support the recent amendment made to these claims. For example, applicant amended the claims **“encrypting the content encryption key using the first decryption information, the first decryption information being**

generated using the provisioning information". So, nowhere in the specification of the provisional or present application discloses these limitations. So according to the specification and original figures of the present and provisional application has no support of the recent amended part. So examiner considers this amendment as a new matter to the claims and necessary action is required.

Response to Arguments

9. Applicant's arguments with respect to claims 1-9, 11-15, 17, and 22-31 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1-9, 11-15, 17, and 22-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Van et al hereinafter Van (US patent 20020090090) in view of Jovanovich et al hereafter Jovanovich (US patent 5703950).

11. As per claims 1, and 11 Van discloses a method comprising steps of: at a broadcaster: distributing first decryption information to the subset of the population of digital receivers, wherein: the first decryption information allows for potentially decrypting a plurality of programs coextensively in time, and the unauthorized digital receivers are cryptographically excluded from using the first decryption information (paragraph 0002); encrypting first content using a first method using a content encryption key distributing the first content (paragraph 0006); encrypting the content encryption key using the first decryption information, the first decryption information being generated using the provisioning information (paragraph, 0004, 0008); and distributing the content encryption key to the subset of the population of digital receivers, wherein the second decryption information is cryptographically secured with the first decryption information (paragraph 0003). Van does not expressly disclose receiving provisioning information from a subset of the population of digital receivers indicating that the subset is potentially within range to receive digital television from the broadcaster. However, in the same field of endeavor, Jovanovich discloses receiving provisioning information from a subset of the population of digital receivers indicating that the subset is potentially within range to receive digital television from the broadcaster (col. 4, lines 35-65) and the first decryption information being generated using the provisioning information (abstract).

Accordingly, it would be obvious to one of ordinary skill in the network security art at the time of invention was made to have incorporated Jovanovich's teachings of using the provisioning information as the decryption information with the teachings of Van, for the purpose of suitably using unique identifier of the sub set to encrypt the encryption key (col. 4, lines 35-65).

12. As per claims 2, Van discloses the method comprising steps of: encrypting second content using a second method that is cryptographically related to third decryption information, wherein at least one of an algorithm, a key and a key length of the second method is different from that of the first method (paragraph 0006); sending the second content; and distributing third decryption information to the subset of the population of digital receivers, wherein the second decryption information is cryptographically secured with the first decryption information (paragraph, 0004).

13. As per claims 3, Van discloses the method a step of uniquely encrypting the first decryption information for each of the subset, wherein the first-listed distributing step comprises sending first description information uniquely encrypted for each of the subset (paragraph 0002).

14. As per claims 4, Van discloses the method comprising a step of determining the unauthorized digital receivers to exclude from the subset of the population of digital receivers (paragraph, 0010).

15. As per claims 5, Van discloses the method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier wherein the first decryption

information is uniquely encrypted for each of the subset (paragraph, 0004).

16. As per claims 6, Van discloses the method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier wherein the first decryption information comprises a key for decrypting the second decryption information (paragraph, 0010).

17. As per claims 7, Van discloses The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier wherein the first decryption information expires by changing keys, key lengths and/or algorithms used to encrypt the first content (paragraph 0017).

18. As per claims 8, Van does not discloses the method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier comprising a step of forwarding the provisioning information to another broadcaster within range of one of the subset. However, Jovanovich discloses where each digital receiver in the population has the unique identifier comprising a step of forwarding the provisioning information to another broadcaster within range of one of the subset (col. 4, lines 35-65).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 8.

19. As per claims 9, Van discloses the method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each

digital receiver in the population has the unique identifier as recited in claim 1, wherein the unique identifier includes a key (paragraph 0006).

20. As per claims 12, and 17 Van discloses a method comprising steps of: at a subset of the population of digital receivers: receiving first decryption information by the subset of the population of digital receivers , wherein: the first decryption information allows for potentially decrypting a plurality of programs coextensively in time, and the unauthorized digital receivers are cryptographically excluded from using the first decryption information; receiving first content (paragraph 0002); receiving content encryption second decryption information from the broadcaster, wherein the content encryption decryption information is encrypted using with the first decryption information (paragraph 0006); and decrypting the first content using the content encryption information, wherein the first decryption information is based on the provisioning information (paragraph, 0004). He does not expressly disclose sending provisioning information from the subset of the population of digital receivers indicating that the subset is within range to receive digital television from a broadcaster. However, Jovanovich discloses sending provisioning information from the subset of the population of digital receivers indicating that the subset is within range to receive digital television from a broadcaster (col. 4, lines 35-65).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 12.

21. As per claims 13, Van discloses the method comprising steps of: receiving second content; receiving third decryption information from the broadcaster, wherein the

third decryption information is cryptographically secured with the first decryption information (paragraph 0006); and decrypting the second content using a second method that is cryptographically related to the third decryption information, wherein at least one of an algorithm, a key and a key length of the second method is different from that of the first method (paragraph, 0004).

22. As per claims 14, Van discloses the method for processing digital television within the population of digital receivers, where each digital receiver in the population has the unique identifier wherein the first decryption information is uniquely encrypted for each of the subset (paragraph 0002).

23. As per claims 15, Van discloses the method for processing digital television within the population of digital receivers, where each digital receiver in the population has the unique identifier wherein the unique identifier includes a key (paragraph, 0010).

24. As per claims 22, Van discloses a content receiver comprising: first decryption information received from a point remote to the content receiver, wherein an unauthorized content receiver is excluded from using the first decryption information; an interface coupled to content signals broadcast to a plurality of content receivers, wherein the content signals carry a plurality of programs coextensively in time (paragraph 0002); second decryption information received from a place remote to the content receiver, wherein the second decryption information is encrypted using the first decryption information (paragraph 0006) ; and first content received with the interface, wherein the first content is decrypted with a method related to the second decryption

information wherein the first decryption information is based on the provisioning information (paragraph 0003). Van does not expressly disclose provisioning information that is sent away from the content receiver for a plurality of content broadcasters coupled to the content receiver. However, Jovanovich discloses provisioning information that is sent away from the content receiver for a plurality of content broadcasters coupled to the content receiver (col. 4, lines 35-65).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 22.

25. As per claims 23-25, Van discloses the content receiver wherein the content signals are protected by a plurality of encryption keys, that is transmitted with digital encoding as recited in claim 23, wherein the first decryption information includes a category key, that is transmitted with digital encoding as recited in claim 22, wherein the first decryption information includes a category key (paragraph, 0010).

26. As per claims 26-28, Van discloses the content receiver wherein the second decryption information includes a content key, that is transmitted with digital encoding wherein the first decryption information expires after a period of time that is transmitted with digital encoding wherein the period of time is two hours, one day, one week, one month, or one year ((paragraphs 0009).

27. As per claims 29-31, Van discloses the content receiver wherein the first decryption information is uniquely encrypted for each of a plurality of content receivers in a system a plurality of content keys, wherein the first content is protected with one of

the plurality of content keys, that is transmitted with digital encoding as recited in claim 30, wherein the first decryption information includes a category key (paragraph 0006).


Conclusion

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad w. Reza whose telephone number is 571-272-6590. The examiner can normally be reached on M-F (9:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, MOAZZAMI NASSER G can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


11/26/07

Mohammad Wasim Reza

AU 2136